REMARKS

The Notice dated January 19, 2005, and the Office Action dated August 27, 2004 have been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto. With regard to the Notice, applicant has underlined the appropriate text in the claims. Applicant hereby resubmits the amendments filed November 18, 2004, and submits these amendments are in compliance with 37 C.F.R. §1.21. Applicant also notes that the following remarks have not been changed from those submitted in the original Response.

Claim 1 is amended to more particularly point out and distinctively claim the subject matter of the invention. No new matter has been added. Thus, claims 1-21 currently are pending in the present application and respectfully are submitted for consideration.

Claims 1-21 were rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent No. 5,991,407 (*Murto*) in view of U.S. Patent No. 5,689,563 (*Brown et al.*). The Office Action took the position that *Murto* teaches all the features of the claims except transmitting at least some of the challenges contained in the authentication data blocks to the terminal, choosing one of the challenges for use in the terminal, and based on this challenge, determining a response and a key to be used with the aid of the subscriber identity module of the terminal, notifying the network with the aid of the data unit of which key corresponding to which challenge was chosen, in determining the authenticator and the check value with the aid of the chosen key. The

Office Action then alleged that *Brown* teaches those features missing from *Murto*. Applicant respectfully submits that the cited references, either alone or in combination, do not disclose or suggest all the features of any of the presently pending claims.

Claim 1, upon which claims 2-9 are dependent, recites an authentication method for telecommunications network. The method includes generating a set of subscriber-specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner as in a known mobile communications system. The method also includes transmitting at least some of the challenges contained in the authentication data blocks to the terminal. The method also includes choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification unit of the terminal essentially in the same way as in a subscriber identification module of the mobile communications system. The method also includes determining an authenticator with an aid of the chosen key in the terminal. The method also includes transmitting from the terminal to the network, the authenticator in a data unit. The data unit contains information relating to the manner in which the authentication is formed and notifying the network of which key corresponding to which challenge was chosen. The method also includes determining a check value with the aid of the chosen key in the network. The method also includes comparing the check value with the authenticator.

Claim 10, upon which claims 11-13 are dependent, recites an authentication system for a telecommunications network. The authentication system includes a terminal of the network, first message transmission means for transmitting an authenticator and a data unit to the network. The data unit includes information relating to the manner in which the authenticator is formed. The authentication system also includes checking means for determining a check value with aid of the data unit. The terminal of the network includes such an identification unit, which receives as input a challenge from which a response and a key are defined essentially in the same manner as in a subscriber identity module of a main mobile communications system. The system also includes generating means for generating authentication data blocks in the same manner as in the mobile communications systems. The authentication data blocks include a challenge, a response and a key. The system also includes transmission means for transmitting challenges contained by the authentication data blocks to the terminal. The terminal includes selection means for selecting one challenge per use. The first message transmission means inserts such a value into the data unit which indicates which key corresponding to which challenge was selected for use in the terminal. The first message transmission means determine the authenticator and the checking means determine the check value based on the selected key.

Claim 14, upon which claims 15-16 are dependent, recites an authentication method for a telecommunications network. The method includes generating a set of subscriber-specific authentication data blocks, each authentication data block containing

a challenge, a response and a key. The method also includes transmitting at least some of the challenges contained in the authentication data blocks to a terminal. The method also includes receiving an authenticator and a data unit containing information relating to a manner in which the authenticator is formed from the terminal. The method also includes determining based on said data unit which challenge was chosen by the terminal. The method also includes determining a check value with a key corresponding to the chosen challenge. The check value is compared with the authenticator.

Claim 17, upon which claims 18 and 19 are dependent, recites an authentication method for a terminal. The method includes receiving a set of challenges from a telecommunications network. The method also includes choosing one challenge from the set of challenges. The method also includes determining a response and a key based on the chosen challenge. The method also includes determining an authenticator based on the key corresponding to the chosen challenge. The method also includes transmitting the authenticator and the data unit to the telecommunications network. The data unit relates to the manner in which the authenticator is formed. The method also includes notifying the telecommunications network of the chosen challenge.

Claim 20 recites a telecommunications network configured to generate a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key. The network also is configured to transmit at least some of the challenges contained in the authentication data blocks to a terminal. The telecommunications network also is configured to receive an authenticator and a data unit

13

containing information relating to a manner in which the authenticator is formed. The telecommunications network also is configured to determine based on the data unit which challenge was chosen by the terminal. The telecommunications network also is configured to determine a check value with the key correspondent to the chosen challenge. The check value is compared with the authenticator.

Claim 21 recites terminal for a telecommunications network. The terminal is configured to receive a set of challenges from a telecommunications network. The terminal is also configured to choose one challenge from a set of challenges. The terminal also is configured to determine a response and a key based on the chosen challenge. The terminal also is configured to determine an authenticator based on the key corresponding to the chosen challenge. The terminal also is configured to transmit the authenticator and the data unit to the telecommunications network. The data unit relating to the manner in which the authenticator is formed and notifying the telecommunications network of the chosen challenge.

As discussed in the specification, examples of the present invention enable the use of the known authentication method of a telecommunications network for producing an authenticator for a terminal. Examples of the present invention enable a terminal to receive a challenge and to determine a corresponding key and response. The response is sent from the terminal to the network, where the response received from the terminal is compared to the response calculated in the network. If these two responses are equal, the terminal is successfully authenticated. Thus, it is possible to share a secret key between

14

the terminal and the network for calculating an authenticator in the terminal and for checking the authenticator network. The authenticator may be calculated using any method, which has been, for example, agreed upon before hand. According to examples of the present invention, the network sends at least some random challenges to the terminal and the terminal chooses one of the available random challenges. The network is notified about the chosen challenge using a data unit. It is respectfully submitted that the cited references, either alone or in combination, fail to disclose or suggest the elements of any of the presently pending claims. Therefore, the cited references fail to provide the critical and unobvious advantages discussed above.

Murto relates to subscriber authentication in a mobile communications system. *Murto* describes an authentication mechanism in a global system for a mobile communications network using A3/A8 algorithms for calculating the response and key from a received challenge. Figure 5 of *Murto* shows a challenge sent to a terminal and the terminal sending an authentication result to the network. A mobile station within *Murto* receives an authentication request and extracts the challenged random number from the message. The mobile station performs computing using a key corresponding to the challenged random number. The result of the computing is a response corresponding to the challenge. The terminal determines the response corresponding to the challenge, and sends the response to the network. Thus, only one challenge is sent at a time according to *Murto*. *Murto*, however, does not disclose or suggest the features of sending at least some challenges to a terminal, choosing the challenge to be used in the terminal,

determining the response and the key based upon the chosen challenge, notifying the network of the challenge which was chosen, and determining an authenticator and a check value based on the chosen challenge. As will be discussed below, *Brown* fails to cure these significant deficiencies.

Brown relates to using instant-specific information in the authentication procedure in addition to random challenges to minimize the number of messages needed in an authentication procedure. A global challenge of *Brown* is a challenge that is broadcast to all terminals in the network. In the authentication procedure, the terminal determines a response based on the global challenge it receives on a broadcasting channel. The global challenge is changed periodically to avoid problems relating to fraudulent use. *Brown* describes using one global challenge at a time and both the terminal and the network being involved in an authentication procedure that uses the current global challenge. *Brown* also describes two options regarding providing a random challenge to the terminal and network in the beginning of the authentication procedure, as shown by step 202 in Figure 2. One option is generating a random challenge in the network and transmitting the random challenge over a common system signal channel to a terminal. Another option of *Brown* is generating a random challenge in the terminal and transmitting the random challenge to the network. The network of *Brown* knows which random challenge the terminal uses in the authentication procedure, either because the network generated the random challenge itself or the network received the random challenge from the terminal in the beginning of the authentication procedure. Thus, *Brown* describes only

one random challenge that is used in a specific authentication procedure. *Brown*, however, does not disclose or suggest choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification unit of the terminal essentially in the same way as in a subscriber identification module of the mobile communication system, determining an authenticator with an aid of the chosen key in the terminal, and transmitting from the terminal to the network the authenticator and a data unit.

In contrast, claim 1 of the present invention recites "choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification unit of the terminal essentially in the same way as in a subscriber identification module of the mobile communications system, determining an authenticator with an aid of the chosen key in the terminal, transmitting from the terminal to the network the authenticator and a data unit, the data unit containing information relating to the manner in which the authentication is formed and notifying the network of which key corresponding to which challenge was chosen." Claim 10 is directed to an authentication system, and recites some common features with claim 1. Claim 14 recites "transmitting at least some of the challenges contained in the authentication data blocks to a terminal, determining based on said data unit which challenges chosen by the terminal, and determining a check value with the key corresponding to the chosen challenge, said check value to be compared with the authenticator." Claim 17 recites "receiving a set of challenges from a

17

telecommunications network, choosing one challenge from the set of challenges, determining the response in the key based on the chosen challenge, and determining an authenticator based on the key corresponding to the chosen challenge." Claim 20 is directed to a telecommunications network, and recites some features in common with claim 14. Claim 21 is directed to a terminal for a telecommunications network, and recites some of the features of claim 17.

As noted above and as admitted in the Office Action, *Murto* does not disclose or suggest all the features of the presently pending claims. Applicant submits that *Brown* does not disclose or suggest these features missing from *Murto*. For example, *Brown* does not disclose or suggest transmitting at least some of the challenges contained in the authentication data blocks to the terminal and choosing one of the challenges for use in the terminal. *Brown* describes using one global challenge at a time so that the terminal and the network involved in an authentication procedure use this single current global challenge. In *Brown*, only one random challenge is used in a specific authentication procedure. This aspect of *Brown* does not disclose or suggest the terminal choosing one of the available random challenges. The cited references also do not disclose or suggest notifying the network about the chosen challenge using the data unit or determining an authenticator and a check value based on the chosen challenge. Instead, *Brown* teaches that the network knows which random challenge the terminal will use in an authentication procedure, as described above. At least these features of the pending claims are not disclosed or suggested by this aspect of *Brown*, either alone or in

combination with *Murto*. Therefore, the cited references, either alone or in combination, do not disclose or suggest all the features of the pending claims.
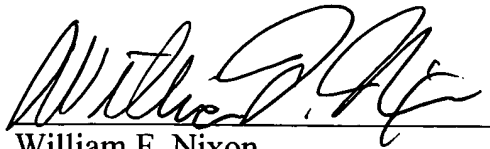
Because the cited references, either alone or in combination, do not disclose or suggest all the features claims 1, 10, 14, 17, 20 and 21, then claims 1-21 are not rendered obvious. The dependent claims also are not disclosed or suggested by the cited references at least because of their dependency upon the independent claims, and the fact that they recite additional subject matter not disclosed or suggested by the cited references. Applicant respectfully requests that the obviousness rejection for claims 1-21 be withdrawn.

It is submitted that each of claims 1-21 recite subject matter that is neither disclosed nor suggested by the cited references, either alone or in combination. It is therefore respectfully requested that all of claims 1-21 be allowed, in this application past to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

William F. Nixon
Registration No. 44,262

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

WFN:cct